UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,689	01/28/2002	David Aro Bruton III	RSW920020011US1	4064

7590 07/26/2006

Jerry W. Henrndon
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,689	BRUTON ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-15,22,24-27,32-40 and 45-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-15,22,24-27,32-40 and 45-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A response to a Notice of Non-Compliant Amendment was received on 27 April 2006. By this response, Claims 1, 3-6, 8, 9, 11-15, 22, 24-27, 32, and 34-40 have been amended. Claims 2, 16-21, 23, 28-31, 33, and 41-44 have been canceled. New Claims 45-58 have been added. Claims 1, 3-15, 22, 24-27, 32, 34-40, and 45-58 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 04 April 2006 have been fully considered but they are not persuasive.

Regarding the rejections of independent Claims 1, 22, and 32 under 35 U.S.C. 102(e) as anticipated by Vaidya, US Patent 6279113, Applicant argues that the amendments to the independent claims "remove any confusion between Vaidya's 'sequential' profiles ... and Vaidya's 'timer/counter'-based profiles" (see page 22 of the response received 04 April 2006). First, the Examiner notes that it is not clear what confusion exists or existed between the sequential and timer/counter profiles, both taught by Vaidya, and therefore the Examiner fails to appreciate this argument.

The Examiner additionally notes that Applicant draws attention, in parenthetical comments, to the fact that the profiles noted in Vaidya "require investigating more than one incoming packet" (see page 22 of the 04 April 2006 response). It is noted that there

is nothing in the claims directed to the number of packets on which intrusion detection is being performed, or how many packets make up the claimed "inbound communications", or, in fact, any explicit mention of packets recited in the claims whatsoever. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Further, Applicant alleges that Vaidya does not teach defining or defined intrusion suspicion levels, associating such defined suspicion levels with set of conditions, defining or defined sensitivity levels, or using sensitivity levels in concert with suspicion levels (see pages 22 and 23 of the 04 April 2006 response). These arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. The arguments merely allege that the noted limitations are not present in the reference but do not provide any evidence in support of such an allegation, and, further, the arguments do not actually point out specific distinctions between how the cited portions of Vaidya allegedly differ from the claims. Further, the Examiner believes that Vaidya does, in fact, disclose the recited limitations, as set forth below.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Claim Objections

3. Claims 1, 22, and 32 are objected to because of the following informalities:

Claims 1 and 22, in lines 6-7 of each claim, and Claim 32, in lines 7-8, each recite "a set of at least one conditions which describe the potential intrusion event". It appears that "conditions" should read "condition" and that "describe" should read "describes".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The rejection of Claim 8 under 35 U.S.C. 112, second paragraph, as indefinite, set forth in the previous Office action, has been overcome by the amendment to the claim. However, the claim remains rejected, and the remaining claims are rejected on a new ground, for the reasons detailed below.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1, 3-15, 22, 24-27, 32, 34-40, and 45-58 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the at least one sets of conditions" in line 14. There is insufficient antecedent basis for this limitation in the claims.

Claim 9 recites the limitation "the defined at least one set of conditions" in lines 1-3. There is insufficient antecedent basis for this limitation in the claims, although it appears that this may be a reference to one of the plurality of defined sets each of at least one condition (defined for each of a plurality of potential intrusion events).

Claim 11 recites the limitation "each of the at least one set of conditions is specified as a condition part in an intrusion detection rule" in lines 1-3. First, there is insufficient antecedent basis for the limitation "the at least one set of conditions". Further, as written, the claim requires that each set be specified as a condition part; however, it appears that it is intended for each condition in each set to be specified as a condition part of a rule.

Claim 22 recites the limitation "the at least one defined sets of conditions" in line 14. There is insufficient antecedent basis for this limitation in the claims. Further, the claim is directed to a system; however, the recited elements of "a plurality of intrusion suspicion levels", "a defined set of at least one conditions", and "a plurality of sensitivity levels" do not appear to have any physical structure such that they would form actual physical components of the recited system. Additionally, in lines 16-19, the limitation of "means for using a currently-applicable one of the defined sensitivity levels..." appears to be only conditionally included in the system; that is, it appears the means for using is only present if any of the sets of conditions are matched (lines 14-16). This is generally unclear and renders the claim indefinite.

Claim 26 recites the limitation "each of the at least one set of conditions is specified as a condition part in an intrusion detection rule" in lines 1-4. First, there is insufficient antecedent basis for the limitation "the at least one set of conditions". Further, as written, the claim requires that each set be specified as a condition part; however, it appears that it is intended for each condition in each set to be specified as a condition part of a rule.

Claim 32 recites the limitation "the at least one sets of conditions" in lines 15-16. There is insufficient antecedent basis for this limitation in the claims. Further, in lines 17-20, the limitation of "computer-readable code for using a currently-applicable one of the defined sensitivity levels..." appears to be only conditionally included in the product; that is, it appears the code for using is only present if any of the sets of conditions are matched (lines 14-16). This is generally unclear and renders the claim indefinite.

Claim 37 recites the limitation "the defined at least one set of conditions" in lines 2-4. There is insufficient antecedent basis for this limitation in the claims, although it appears that this may be a reference to one of the plurality of defined sets each of at least one condition (defined for each of a plurality of potential intrusion events).

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 3-15, 22, 24-27, 32, 34-40, and 45-58 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya, US Patent 6279113.

In reference to Claim 1, Vaidya discloses a method of intrusion detection in a network, where a plurality of intrusion suspicion levels are defined for inbound communications; defining a set of conditions describing each potential intrusion event; associating a suspicion level with each set of conditions; defining a plurality of sensitivity levels for filtering intrusion events; and performing intrusion detection by determining if any of the conditions are matched and if so, using an applicable sensitivity level to determine if the particular inbound communication should be treated as an intrusion event (see column 7, line 52-column 8, line 39, noting that higher sensitivity to certain actions with different levels of suspicion, depending on the previous conditions met in a "sequential" profile, or on the timing and count values in a "timer/counter" profile, will make detection of an attack more likely; for example, if a first condition has been met in a sequential profile, column 7, lines 52-67, then the sensitivity level is raised for the next

packets, and if those packets have an appropriate suspicion level, column 8 lines 1-15, then an intrusion event is detected; noting further that there are a plurality of intrusion and sensitivity levels defined depending on the profiles used).

In reference to Claims 3 and 4, Vaidya further discloses comparing conditions in the computing device, specifically contents of the particular inbound communication, to predetermined conditions signaling a potential intrusion (column 5, lines 27-33).

In reference to Claim 5, Vaidya further discloses that conditions can include the state of a protocol stack (column 7, lines 18-24; column 8, lines 40-56).

In reference to Claims 6-8, Vaidya further discloses taking defensive actions when it is determined that the inbound communication should be treated as an intrusion, where the defensive actions are determined from policy information stored in a repository (column 6, lines 18-26; column 5, lines 27-33).

In reference to Claims 45-48, Vaidya further discloses that the defensive actions are specified in a rule (column 6, lines 18-21, where the reaction depends on the nature of the attack) and defensive actions can include discarding the inbound communication or limiting traffic associated with a connection (column 6, lines 21-24).

In reference to Claims 49-53, Vaidya further discloses that the defensive action can include reporting the intrusion event can be reported to an entity, by alerting an external management component, writing a record to a log, or recording a trace (column 6, lines 18-26).

In reference to Claims 9 and 10, Vaidya further discloses that the conditions can represent an attack signature, where a signature can represent a class of attacks (column 6, lines 27-40).

In reference to Claim 11, Vaidya further discloses the signatures as conditions to be fulfilled in detection rules, where the rules also include actions to be taken in response to detection of an intrusion event (column 5, lines 33-39; column 6, lines 18-26).

In reference to Claims 12 and 13, Vaidya further discloses operation within layer-specific logic in a protocol stack (column 7, lines 18-26).

In reference to Claim 14, Vaidya further discloses operation in a network analysis device (column 5, lines 18-26).

In reference to Claim 15, Vaidya further discloses consulting a stored mapping between the sensitivity levels and suspicion levels to determine if the inbound communication should be treated as an intrusion event (see column 7, line 52-column 8, line 39, noting that higher sensitivity to certain actions with different levels of suspicion, depending on the previous conditions met in a "sequential" profile, or on the timing and count values in a "timer/counter" profile, will make detection of an attack more likely; note also column 5, lines 27-33 where a plurality of profiles are defined).

In reference to Claims 54 and 56, Vaidya further discloses a condition specifying a current system state or a state transition (column 4, lines 8-18).

In reference to Claim 55, Vaidya further discloses a condition specifying a threshold reached (column 4, lines 19-27).

In reference to Claims 57 and 58, Vaidya further discloses that sensitivity can be specified by an administrator or by stored configuration data (column 5, lines 47-67).

Claims 22 and 24-27 are directed to a system and recite limitations corresponding to those recited in Claims 1, 3, 6, 7, 9, 11, and 15, and are rejected by a similar rationale.

Claims 32 and 34-40 are directed to a software implementation and recite limitations corresponding to those recited in Claims 1, 3-7, 9, 10, 12, 14, and 15, and are rejected by a similar rationale.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Pearson, US Patent 6990591, discloses a system including an intrusion detector using attack signatures and having a remote monitoring center.

b. Moran, US Patent 6996843, discloses a network intrusion detection system including the use of suspicion levels assigned to events.

c. Parekh et al, US Patent 7058821, discloses a system for detecting intrusion attacks in network packets, using attack signatures and rules based (at least) on the state of a protocol stack.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAY
zad

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100